

## REMARKS

Claim 1 has been amended to overcome the Section 101 rejection. Specifically, "determining" is now modified by "using snooping," which clearly indicates an electronic process undertaken at the now recited hardware server. "Selecting" is also specified as being done in that hardware server. Downloading occurs from the server to a protocol in a central office infrastructure. The fingerprint control protocol is then transferred from the infrastructure to the terminal whose characteristics were provided to the front end via snooping to enable the selection of the appropriate algorithm and control parameters.

Therefore, the Section 101 rejection is overcome with respect to claims 1-8.

With respect to the objection to claims 17 *et seq.*, the language in paragraph 13 of the specification has been removed to prevent any reading of machine readable medium as including waves.

Therefore, reconsideration of the rejection of those claims is requested.

With respect to the rejection based on prior art, the reliance on Agnihotri is not understood. The claimed invention relates to a system for snooping the terminal mode characteristics and, based on that snooping, selecting the appropriate algorithm and control parameters for processing a fingerprint at the terminal end. Nothing of the sort is done in Agnihotri. Instead, all he is concerned about is determining where commercials are in a video stream. Its applicability to the claimed invention is obtuse to say the least. There is no server in Agnihotri, nor has the office action indicated one. Therefore, there is no snooping at the server, and there is no snooping at the server to determine terminal characteristics. There is no selecting of an algorithm or control parameters for processing a fingerprint whatsoever. The rest of the limitations are similarly inapplicable. Thus, the reason for citing Agnihotri is not understood.

Nor does Dorai remedy this situation. The cited material in column 7 has nothing to do with snooping, from a server, characteristics of a terminal node. The items 220, 230, and 240 referred to therein are cell phones which could not correspond to servers and could not correspond to snooping from the characteristics of terminal nodes. Nor is there any selecting an algorithm based on such snooping. Therefore, it is not seen how Dorai has anything to do with the claimed invention. The combination of Dorai and Agnihotri do not even have anything to do with


fingerprints, much less snooping characteristics from a server of a terminal in order to figure out what algorithm and control parameters to download.

It is contended that Schrempp teaches a method for transferring a fingerprint control protocol to a terminal node. It does not appear that anything in Figure 6 or paragraph 49 suggests such a thing. For example, block 630 simply determines whether the fingerprint matches and, if so, obtain information and, otherwise, add a fingerprint to request. There is no suggestion of any fingerprint control protocol or any transfer to a terminal node. Thus, reconsideration is requested for this additional reason.

*A prima facie* rejection is not made out and reconsideration is requested.

Respectfully submitted,

Date: February 19, 2009



---

Timothy N. Trop, Reg. No. 28,994  
TROP, PRUNER & HU, P.C.  
1616 South Voss Road, Suite 750  
Houston, TX 77057-2631  
713/468-8880 [Phone]  
713/468-8883 [Fax]

Attorneys for Intel Corporation